APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/690,243	10/17/2000	Ari Engelberg	36530/RRT/S850	2962

23363	7590	06/21/2004

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER
BACKER, FIRMIN

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 06/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/690,243	ENGELBERG ET AL.
	Examiner	Art Unit
	Firmin Backer	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>05 April 2004</u> .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-79</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-79</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>17 October 2000</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4)☐ Interview Summary (PTO-413) Paper No(s). _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: .

Response to Amendment

This is in response to an amendment file on April 5th, 2004 for letter for patent filed on October 17th, 2000 in which claims 1-79 were presented for examination. In the amendment, claims 1 and 39 have been amended. Claims 1-79 remain pending in the letter.

Claim Rejections - 35 USC § 103

1.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.   Claims 1-79 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whitehouse (U.S. Patent No. 6,005,945 (*applicant submitted IDS*)) in view of Lewis et al (U.S. Patent No. 6,233,565).

3.   As per claim 1, Whitehouse teaches a scalable on-line system for printing value bearing items (VBI) (*electronic distribution of postage, 100*) comprising a client system (*host system, fig 3*) for interfacing with one or more users (*customer, 104*) and a scalable server system (*postal service, 180*) capable of communicating with the client system over a communication network (*network, fig 3*) (*see figs 3, 4, column 7 line 54-8 line 11*) comprising a database (*secure central computer 102, memory 154*) remote from the users including information about the users (*see fig 4, column 8 lines 23-29, 54-58, 9 line 15-19*), and a plurality of security device transaction data

(transaction log) stored in the database for ensuring authenticity of the one or more users,

wherein each security device transaction data can be processed in the server system in a stateless

manner *(see figs 3, 4, column 8 line 59-65, 9 line 12-50)*. Whitehouse fails to teach an inventive

concept with a stateless cryptographic module for authenticating the one or more users. However

Lewis et al teach an inventive concept with a stateless cryptographic module for authenticating

the one or more users *(see fig 8 column 23 lines 66-26 line 12)*. Therefore, it would have been

obvious to one of ordinary skill in the art the invention was made to modify the inventive

concept of Whitehouse to include Lewis et al's a stateless cryptographic module for

authenticating the one or more users because this would have enhance the security of the system.

4.   As per claim 2, Whitehouse teaches a system wherein each security device transaction

data is related to a user *(see column 9 lines 12-20)*.

5.   As per claim 3, Whitehouse teaches a system wherein the security device transaction data

related to a user is loaded into the cryptographic module when the user requests to operate on a

value bearing item *(see column 9 lines 45-50)*.

6.   As per claim 4, Whitehouse teaches a system wherein the security device transaction data

related to a user is updated and returned to the database *(see column 9 line 51-63, 12 line 53-56)*.

7.   As per claim 5, Whitehouse teaches a system further comprising one module is capable

of processing any of the plurality of security device transaction data *(see column 9 line 51-63)*.

8.   As per claim 6, Whitehouse teaches a system wherein a user can be authenticated using

any of the cryptographic modules (*see column 9 line 51-63*).

9.   As per claim 7, Whitehouse teaches a system further comprising computer executable

code for load-balancing to route user requests to the at least one more cryptographic module (*see

column 19 line 35-20 line 8*).

10.   As per claim 8, Whitehouse teaches a system further comprising computer executable

code for load-balancing to distribute traffic among the multiple cryptographic modules (*see

column 19 line 35-20 line 8*).

11.   As per claim 9, Whitehouse teaches a system wherein the cryptographic module is

capable of authenticating any of the one or more users (*see column 19 line 35-20 line 8*).

12.   As per claim 10, Whitehouse teaches a system wherein the database is partitioned across

a plurality of physical databases (*see fig 7*).

13.   As per claim 11, Whitehouse teaches a system wherein the cryptographic module

performs cryptographic function on a transaction related to the database (*see fig 7*).

14.   As per claim 12, Whitehouse teaches a system further comprising computer executable code for password authentication to prevent unauthorized access to the database (*see column 10 line 45-60*).

15.   As per claim 13, Whitehouse teaches a system wherein the database stores a first set of one or more last database transactions and the cryptographic module stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction (*see column 8 line 63-9 line 12*).

16.   As per claim 14, Whitehouse teaches a system wherein the cryptographic module prevents further database transactions if the second set of one or more last transaction stored in the cryptographic module does not compare with the first set of one or more last transaction stored in the database (*see column 9 lines 1-12*).

17.   As per claim 15, Whitehouse teaches a system wherein the cryptographic module includes a data validation subsystem for allowing the module to verify that data is up to date and an auto-recovery subsystem for automatically re-synchronize the module with the data (*see column 9 line 32-50*).

18.   As per claim 16, Whitehouse teaches a system wherein the cryptographic module

includes a computer executable code for preventing unauthorized modification of data (*see*

column 15 line 1-17).

19.   As per claim 17, Whitehouse teaches a system wherein the cryptographic module

includes a computer executable code for ensuring the proper operation of cryptographic security

and VBI related meter functions (*see column 16 line 45-67*).

20.   As per claim 18, Whitehouse teaches a system wherein the cryptographic module

includes a computer executable code for supporting multiple concurrent users (*see fig 7*).

21.   As per claim 19, Whitehouse teaches a system wherein the database includes one or more

indicium data elements, data for account maintenance, and data for revenue protection (*see fig

4*).

22.   As per claim 20 and 21, Whitehouse teaches a system wherein the database includes

virtual meter information and a descending register data (*see column 10 line 50-11 line 26, 14*

lines 25-36).

23.   As per claims 22 and 23, Whitehouse teaches a system wherein the value bearing item is

a mail piece that comprises a digital signature (*see column 7 lines 1-5, 8 line 47-51 and 11 lines*

27-29.

24.   As per claim 24, Whitehouse teaches a system wherein the cryptographic module

performs cryptographic function on validation information according to a user request for

printing a VBI (*see column 9 lines 12-30*).

25.   As per claim 25, Whitehouse teaches a system wherein the cryptographic module

generates data sufficient to print a postal indicium in compliance with postal service regulation

on a mail piece (*see column 8 line 65-9 line 11*).

26.   As per claims 26-31, Whitehouse teaches a system wherein a bar code is printed on the

value bearing item that is a ticket, is a coupon, is currency, a voucher, a traveler's check (*see*

column 8 lines 14-18, 13 lines 56-60).

27.   As per claim 32, Whitehouse teaches a system wherein each security device transaction

data includes one or more of an ascending register value, a descending register value, a

respective cryptographic module ID, an indicium key certificate serial number, a licensing ZIP

code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets,

date and time of last transaction, last challenge received from a respective client subsystem, an

operational state of the respective module, expiration dates for keys, and a passphrase repetition

list (*see column 9 lines 12-67, 13 lines 20-36, 14 lines 25-55*).

28.   As per claim 33, Whitehouse teaches a system wherein each security device transaction data includes one or more of a private key, a public key, and a public key certificate, wherein the private key is used to sign module status responses and a VBI which, in conjunction with a public key certificate, demonstrates that the module and the VBI are authentic (*see column 9 lines 12-50, 13 lines 20-36*).

29.   As per claim 34, Whitehouse teaches a system wherein the cryptographic module is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (*see column 23 lines 49-59*).

30.   As per claim 35, Whitehouse teaches a system wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem (*see figs 3 and 4*).

31.   As per claim 36, Whitehouse teaches a system wherein the database includes one or more of a postal database, a provider database, an e-commerce database, and a membership database (*see fig 3, 4*).

32.   As per claim 37, Whitehouse teaches a system further comprising an address matching

server for verifying a correct address specified by a user (*see column 12 line 65-13 line 15*).

33.   As per claim 38, Whitehouse teaches a system further comprising a printer driver

database for storing supported printer driver information (*see figs 3 and 4*).

34.   As per claim 39, Whitehouse teaches a method for printing value-bearing items (VBI)

(*electronic distribution of postage, 100*) via a communication network (*network, fig 3*) including

a client system (*host system, fig 3*), and a scalable server system (*postal service, 180*) (*see figs 3,

4, column 7 line 54-8 line 11*), the method comprising interfacing (*communicating*) with one or

more users (*customer, 104*) via the client system (*host system, fig 3*) communicating with the

client system over the communication network(*see figs 3, 4, column 7 line 54-8 line 11*), storing

(*storing*) user information (*user information*) in a database (*secure central computer 102,

memory 154*) accessible through the network (*see fig 4, column 8 lines 23-29, 54-58*), and storing

in the database a plurality of security device transaction data for ensuring authenticity of the one

or more users, wherein each security device transaction data can be processed in the server

system in a stateless manner (*see figs 3, 4, column 8 line 59-65, 9 line 12-50*). Whitehouse fails

to teach an inventive concept authenticating the one or more users using a scalable cryptographic

module. However, Lewis et al teach an inventive concept authenticating the one or more users

using a scalable cryptographic module (*see fig 8 column 23 lines 66-26 line 12*). Therefore, it

would have been obvious to one of ordinary skill in the art the invention was made to modify the

inventive concept of Whitehouse to include Lewis et al's an inventive concept authenticating the

one or more users using a scalable cryptographic module because this would have enhance the

security of the system.

35.   As per claim 40, Whitehouse teaches a method wherein each security device transaction

data is related to a user (*see column 9 lines 12-20*).

36.   As per claim 41, Whitehouse teaches a method further comprising of loading the security

device transaction data related to a user into the cryptographic module when the user requests to

operate value bearing item (*see column 9 lines 45-50*).

37.   As per claim 42, Whitehouse teaches a method further comprising of updating and

returning the security device transaction data related to a user to the database (*see column 9 line

51-63, 12 line 53-56*).

38.   As per claim 43, Whitehouse teaches a method further comprising adding at least one

more stateless cryptographic module, wherein each cryptographic module is capable of

processing any of the plurality of security device transaction data (*see column 9 line 51-63*).

39.   As per claim 44, Whitehouse teaches a method further comprising of authenticating a

user using any of the cryptographic modules (*see column 9 line 51-63*).

40.   As per claim 45, Whitehouse teaches a method further comprising load-balancing to route user requests to the at least one more cryptographic module *see column 19 line 35-20 line 8)*.

41.   As per claim 46, Whitehouse teaches a method further comprising load-balancing to distribute traffic among the multiple cryptographic modules *see column 19 line 35-20 line 8)*.

42.   As per claim 47, Whitehouse teaches a method further comprising authenticating any of the one or more users using the cryptographic module *(see column 9 line 51-63)*.

43.   As per claim 48, Whitehouse teaches a method comprising partitioning the database across a plurality of physical databases *(see fig 7)*.

44.   As per claim 49, Whitehouse teaches a method further comprising encrypting database transactions using the cryptographic module *(see column 10 line 45-60)*.

45.   As per claim 50, Whitehouse teaches a method further comprising verifying a user password before granting access to the database *(see column 15 line 1-17)*.

46.   As per claim 51, Whitehouse teaches a method further comprising storing one or more last database transactions in the database storing one or more last database transactions in the cryptographic module; and comparing the one or more last database transactions stored in the

database with the one or more last database transactions stored in the cryptographic module to

verify each database transaction (*see column 16 line 45-67*).

47.   As per claim 52, Whitehouse teaches a method further comprising encrypting

transactions related to the database using the cryptographic module (*see column 15 line 1-17*).

48.   As per claim 53, Whitehouse teaches a method further comprising storing one or more

last database transactions in the database, storing one or more last database transactions in the

cryptographic module for comparison with the one or more last database transactions stored in

the database to verify each database transaction (*see column 10 line 45-60*).

49.   As per claim 54, Whitehouse teaches a method further comprising preventing further

database transactions if the one or more last transaction stored in the cryptographic module does

not compare with the one or more last transaction stored in the database (*see column 8 line 63-9*

line 12).

50.   As per claim 55, Whitehouse teaches a method further comprising preventing

unauthorized modification of data using the cryptographic module (*see column 16 line 45-67*).

51.   As per claim 56, Whitehouse teaches a method further comprising verifying that the

database is up to date (*see column 10 line 45-60*).

52.   As per claim 57, Whitehouse teaches a method further comprising automatically re-synchronizing the cryptographic module with the database (*see column 9 line 51-63*).

53.   As per claim 58, Whitehouse teaches a method further comprising ensuring the proper operation of cryptographic security and VBI related meter functions (*see column 9 lines 12-20*).

54.   As per claim 59, Whitehouse teaches a method further comprising supporting multiple concurrent operators (*see fig 7*).

55.   As per claim 60, Whitehouse teaches a method further comprising storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices, storing a table including the information about a last transaction in the database, comparing the information saved in the respective device with the respective information saved in the database; and loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database (*see column 10 line 45-11 line 25*).

56.   As per claim 61, Whitehouse teaches a method further comprising the step of storing data for creating one or more indicium, account maintenance, and revenue protection (*see column 10 line 45-11 line 25*).

57.   As per claims 62-65, Whitehouse teaches a method further comprising printing a mail piece includes a digital signature, a postage amount, an ascending register of used postage and descending register of available postage (*see column 13 lines 20-40, 14 line 25-36, 16 lines 19-38*).

58.   As per claims 66-71, Whitehouse teaches a method further comprising printing a ticket, a bar code, a coupon, currency, a voucher, a traveler's check (*see column 7 line 46-53, 8 line 14-18, 13 lines 56-60*).

59.   As per claim 72, Whitehouse teaches a method wherein the security device transaction data includes an ascending register value, a descending register value, a respective cryptographic device ID, an indicium key certificate serial number, a licensing ZIP code, a key token for an indicium signing key, user secrets, a key for encrypting user secrets, date and time of last transaction, last challenge received from a respective client subsystem, an operational state of the respective device, expiration dates for keys, and a passphrase repetition list (*see column 13 lines 20-40, 14 line 25-36, 16 lines 19-38*).

60.   As per claim 73, Whitehouse teaches a method further comprising performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption, DES, Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms using each of the cryptographic devices (*see 23 lines 49-59*).

61.   As per claim 74, Whitehouse teaches a method further comprising keeping track of user

accesses to a vendor website using a website database (*see fig 7*).

62.   As per claim 75, Whitehouse teaches a method further comprising storing postal

transaction data, financial transaction data, customer marketing information, commerce product

information, meter license information, meter resets, meter history, and meter movement

information in an offline database (*see column 10 line 45- 11 line 29*).

63.   As per claim 76, Whitehouse teaches a method further comprising storing customer

information, financial transactions, and information for marketing queries in a data warehouse

database (*see column 9 lines 12-31*).

64.   As per claim 77, Whitehouse teaches a method further comprising authorizing and

capturing funds from a customer's account and transferring the funds to a vendor's account using

an e-commerce server (*see column 11 line 60-67*).

65.   As per claim 78, Whitehouse teaches a method further comprising verifying a correct

address specified using a user using an address matching server (*see column 9 line 51-63, 12 line

53-56*).

66.   As per claim 79, Whitehouse teaches a method further comprising storing supported

printer driver information in a printer driver database (*see figs 3 and 4*).

Response to Arguments

67.   Applicant's arguments filed April 5th, 2004 have been fully considered but they are not persuasive.

Applicants argue that the prior art (Whitehouse and Lewis) fail to teach an inventive concept wherein a "stateless cryptographic module for authenticating users and for processing value for the user." Examiner respectfully disagrees with applicant's characterization of the prior art. Lewis et al teach an authentication service that is responsible for authenticating each client with the server. The client has no direct control over the services performed by the server cryptographic module. All services performed by the server cryptographic module are under the direct control of a Transaction "Manager" server. Once the client has been authenticated, it submits a transaction request to the transaction server and waits for a response. The Transaction Manager process the transaction and return a "receipt" to the client. All transaction "receipts" will contain a date/time stamp, and a sequence number (*value*) and a digital signature to verify the authenticity of a transaction in relation to other similar transactions. *For instance, for a given customer, the sequence number will increase by one each time until a threshold is met, e.g., 10,000, at which point the counter will reset to 1 (emphasis added)*. Furthermore, the transaction Manager embodies the logic required to complete a transaction while enforcing the security and integrity of the server cryptographic module. Based on the authenticated user, the transaction requested, the date/time stamp, and the sequence number, the Transaction Manger would determine whether the requested transaction is valid. The Transaction Manager will complete the

transaction by sending a receipt, including a digital signature as evidence of payment for the transaction, back to the client 2n. In the case of the postage purchase system, the receipt is the indicium, which includes the foregoing and the postage related information (addresse, postage amount, etc.).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

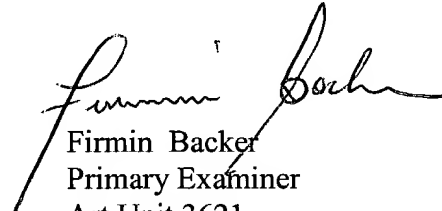A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firmin Backer
Primary Examiner
Art Unit 3621

June 14, 2004